Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-40 are pending in the application, with claims 1, 7, 15, 16, 23, 24, 29, and 30 being the independent claims. Claim 15 is sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

It is requested that this response be entered after a final rejection because the amendments are only made for clarification, and do not substantively change the combinations being claimed. The only amendment being made corrects a typographical error and does not substantively change the claim. Thus, the same issues are presented for reconsideration, not requiring any further search by the Examiner. In view of the amendments proposed to the claims, Applicants believe this application should be in better condition for allowance or appeal after this response is entered.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Examiner's Response to Arguments

The Examiner, in response to Applicants' previous arguments, on page 3 of the Final Office Action ("the Office Action") states:

> There is no disclosure to modify the access requirements by the resolution authority in the specification of the original claims. See the 112 rejection.

Applicants respectfully disagree. As it will be explained in more detail with respect to rejections of claims 1, 7, 15, 16, 23, 24, 29, and 30 under 35 U.S.C. § 112, in one example, paragraph [0033] of the originally filed Specification states "*submitting, by the controller, a request for authorization to* ***a resolution authority, which is configured to modify the one or more access requirements****, in response to a comparison that indicates that access by the access candidate is prohibited.*" This language is recited in claim 1 and similar language is recited in claims 7, 15, 16, 23, 24, 29 and 30.

The Examiner, in response to Applicants' previous arguments, on page 4 of the Office Action states:

> The Timson prior art discloses the capability to add additional authentication modules to the authentication procedures. These additional authentication modules can generate a hierarchical structure for the authentication process with access to the resolution authority performed as a last authentication process as per claim limitation. (see Timson col 4, line 60 - col. 5, line 4: hierarchical authorization structure)

Applicants respectfully disagree. As it will be explained in more detail with respect to rejection of claims 1-4, 16-19, 24-26, 29, and 38-40, Timson discloses that a set of data operations may be stored on a controllable module. Other types of modules such as interrogatable module (IM) and enable module (EM) can be made from the controller module by writing permissions data to the modules. In this manner, hierarchical sets of permissions for data operations can be written to the modules (Timson Col. 4, Line 60 to Col. 5, Line 4). Although Timson teaches that other types of modules such as EM or IM can be made (that might have hierarchical permissions), the hierarchical data system is implemented in the form of ***dual secure data module scheme*** (Timson Col. 11, Line 65 to Col. 12, Line 4). Therefore, there is no teaching or suggestion in Timson that the authentication procedure (or access determination) can use additional authorization modules as the Examiner states in the Office Action.

Rejections under 35 U.S.C. § 112

<u>Claims 1, 7, 15, 16, 23, 24, 29 and 30</u>

The Examiner rejected claims 1, 7, 15, 16, 23, 24, 29 and 30 under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement. Applicants respectfully traverse this rejection.

The Examiner, on pages 4 and 5 of the Office Action, states:

> There is no disclosure for: the resolution authority, which is configured to modify the one or more access requirements". There is no disclosure for a resolution authority to modify access requirements in the specification or the original claims.

Applicants respectfully disagree. As an example, paragraph [0033] of the originally filed Specification says "*submitting, by the controller, a request for authorization to* ***a resolution authority, which is configured to modify the one or more access requirements****, in response to a comparison that indicates that access by the access candidate is prohibited.*" This language is used in claim 1 and similar language is used in claims 7, 15, 16, 23, 24, 29 and 30.

Accordingly Applicants respectfully request that the Examiner reconsider and withdraw this rejection.

Rejections under 35 U.S.C. § 103

<u>Claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, and 37-40</u>

The Examiner rejected claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, and 37-40 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,041,412 to Timson *et al.* ("Timson") in view of U.S. Patent No. 6,959,336 to Moreh *et al.* ("Moreh"). Applicants respectfully traverse this rejection.

<u>Claims 1-4, 16-19, 24-26, 29, and 38-40</u>

The Examiner contends that the combination of Timson and Moreh teaches each of the elements of independent claims 1, 16, 24, and 29. Applicants respectfully disagree. Claim 1 recites:

> A method for providing an access candidate access to secured electronic data, the method comprising:
>
> receiving a request for access candidate access to the secured electronic data by a controller associated with the secured electronic data;
>
> comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data;
>
> ***submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited; and***
>
> granting the access candidate access to the secured electronic data if the resolution authority provides authorization for such access.

Applicants maintain that the combination of Timson and Moreh does not teach or suggest each and every feature of claim 1. For example, the combination of Timson and Moreh does not teach or suggest "*submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited*" as recited in claim 1.

First, as discussed in the reply filed July 2, 2008, Timson discloses an apparatus and a method for providing access to secured data or area that includes at least two secure data modules, an interrogatable module (IM) and an enable module (EM). In the case that EM does not have appropriate permissions, no data communication is allowed and also if the EM does not provide the necessary permissions, the IM prevents the EM to access the requested data (Timson column 3, line 11 to column 4, line 15, and also column 13, line 22 to column 14, line 40).

The Examiner, on page 6 of the Office Action, states:

> Timson discloses access determination using additional authorization modules. (see Timson col 4, line 60 - col. 5, line 4: additional authorization modules). Timson does not specifically disclose a resolution authority or a 3rd party providing authentication service.

Applicants respectfully disagree. Timson discloses that a set of data operations may be stored on a controllable module. The controller module can be configured as other types of modules, such as EM or IM, by writing permissions data to the modules. In this manner, hierarchical sets of permissions for data operations can be written to the modules (Timson Col. 4, Line 60 to Col. 5, Line 4). Therefore, although Timson teaches that other types of modules such as EM or IM can be made (that might have hierarchical permissions), but the hierarchical data system is implemented in the form of ***dual secure data module scheme*** (Timson Col. 11, Line 65 to Col. 12, Line 4). Therefore, there is no teaching or suggestion in Timson that the authentication process (or access determination) can use additional authorization modules as the Examiner states in the Office Action. The authentication process of Timson only involves one EM and one IM that communicate with each other to provide access to secured data and no additional security level could be added to this authentication process and if either of EM or IM does not have the necessary permissions, access to the secured data is denied. Therefore, Applicants maintain that Timson and Moreh cannot be combined to establish a prima facie case of obviousness because Timson merely teaches a dual secure data module scheme and contrary to the Examiner's suggestion, there is no teaching or suggestion in Timson that additional layers of authentication services can be added to this dual scheme.

Second, assuming *arguendo* that it is proper to combine these references in the manner suggested, with which Applicants do not acquiesce, the Examiner, on page 6 of the Office Action, states that Timson does not disclose a resolution authority. However, the Examiner relies upon Moreh (Moreh Col. 2, Lines 48-62; Col. 5, Line 56 to Col. 6, Line 19) to allegedly show the resolution authority feature of claim 1:

> Timson does not specifically disclose a resolution authority or a 3rd party providing authentication services. However, Moreh discloses a resolution authority, which is configured to modify the one or more access requirements. (see Moreh col. 2, lines 48-62; col. 5, line 56 - col. 6, line 19: authentication service between client and server using intermediate entity (protocol proxy))

Applicants maintain that the combination of Timson and Moreh fails to teach all the elements of claim 1 and similarly worded claims 16, 24, and 29 for at least the following reasons. For example, using similar language, claims 1, 16, 24, and 29 all require submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited.

Moreh discloses a system and a method to efficiently maintain security in information systems when multiple authentication types and sources are used (Moreh Col. 1, Lines 17-19). In the Moreh method, a *subject*, who must authenticate itself, uses a *client* to initiate the process of obtaining access to a server application. The client communicates an authentication request for access to the server application to a *protocol proxy*. The *protocol proxy* translates the authentication request into a native protocol of an authentication mechanism and communicates the translated request to the authentication mechanism. Upon successful authentication, the protocol proxy receives a response from the authentication mechanism including attributes and access rights of the subject. Then the protocol proxy creates a name assertion (a type of credential), translate this into an authentication response, and transmits it back to the client. The client delivers the authentication response to the server application.

Therefore, the protocol proxy of Moreh is only used between the client and the authentication mechanism to receive from the authentication mechanism a response including attributes and access rights of the subject and creates an authentication name assertion allowing the client to access the server application (Moreh Col. 6, Lines 7-19 and Col. 2, Lines 57-62). This is not the same as *submitting, by the controller, a request for authorization to* ***a resolution authority, which is configured to modify the one or more access requirements****, in response to a comparison that indicates that access by the access candidate is prohibited,* as recited in claim 1 and similarly worded claims 16, 24, and 29. In contrast to the protocol proxy of Moreh that merely receives attributes and access rights of the subject, claim 1 recites that resolution authority, which is configured to modify the one or more access requirements.

Further, Moreh teaches that upon successful authentication, the protocol proxy receives back from the authentication mechanism a response including attributes and access rights of the subject (Moreh Col. 6, Lines 7-19 and Col. 2, Lines 57-62). In contrast, claim 1 recites *submitting, by the controller, a request for authorization to a* *resolution authority, which is configured to modify the one or more access requirements,* ***in response to a comparison that indicates that access by the access candidate is prohibited****.*

Therefore, for at least the above reasons, the combination of Timson and Moreh fails to disclose all features of independent claim 1. Independent claims 16, 24, and 29 are patentable for similar reasons.

In addition, the Examiner rejected claims 2-4, 18, 19, 25, 26, and 38-40 as being anticipated by the combination of Timson and Moreh. These dependent claims necessarily include all features of their respective independent (claims 1, 16, and 24) and any intervening claims. As discussed above, the combination of Timson and Moreh fails to disclose all features of claims 1, 16, 24, and 29, therefore, claims 2-4, 18, 19, 25, 26, and 38-40 are not anticipated by the cited references.

Also, Applicants assert that the dependent claims 38-40 are patentable over the applied references in view of their respective additional combinations of distinguishing features. For example, at least the "granting a waiver of the one or more access requirements associated with the secured electronic data" feature recited in claim 38, at least the "modifying the one or more access requirements associated with the secured electronic data" feature recited in claim 39, and at least the "excluding the electronic data assigned to one or more prohibited data classes from access by the access candidate" feature recited in claim 40 are not explicitly or implicitly taught or suggested by the applied references. In contrast, in the case where there is conflict between EM or IM's permissions and the requirements, Timson's system prevents data communication or data access. There is absolutely no attempt to resolve the conflict in Timson's system.

Moreover, the protocol proxy of Moreh only authenticates the client and in case of a successful authentication, creates an authentication name assertion allowing the client to access the server application.

Claims 7-10, 14, 30-33, and 37

The Examiner rejected independent claims 7 and 30 as being anticipated by the combination of Timson and Moreh. These independent claims contain similar language to that found in claims 1, 16, 24 and 29, discussed above, and are patentable for the same reasons discussed above. Dependent claims 8-10, 14, 31-33, and 37 necessarily include all features of claims 7 and 30, respectively. The combination of Timson and Moreh fails to disclose all features of claims 7 and 30, therefore claims 8-10, 14, 31-33, and 37 are not anticipated by the combination of Timson and Moreh.

Claims 5, 6, 11-13, 15, 20-23, 27, 28, and 34-36

The Examiner rejected claims 5, 6, 11-13, 15, 20-23, 27, 28, and 34-36 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Timson in view of Moreh and further in view of U.S. Patent Publication No. 2004/0049687 to Orsini *et al.* ("Orsini"). Applicants respectfully traverse this rejection.

Independent claims 15 and 23 contain similar language to that found in claims 1, 7, 16, 24, and 29 and are patentable over the combination of Timson and Moreh for the same reasons discussed above. Further, Orsini fails to cure the deficiencies of the combination of Timson and Moreh as noted above. Orsini does not teach what is missing from the combination of Timson and Moreh, for example the resolution authority, which is configured to modify access requirements (as is disclosed in claims

15 and 23). Therefore, claims 15 and 23 are patentable over Timson, Moreh, and Orsini taken alone, or in combination, for at least the reasons provided above.

In addition, the Examiner rejected claims 5, 6, 11-13, 20-22, 27, 28, and 34-36 as allegedly being unpatentable over the combination of Timson and Moreh and further in view of Orsini. These dependent claims necessarily include all features of their respective independent and any intervening claims including claims 1, 7, 16, 24, and 30, respectively. As discussed above, the combination of Timson and Moreh fails to disclose all features of claims 1, 7, 16, 24, and 30, and further, Orsini fails to cure the deficiencies of the combination of Timson and Moreh as noted above. Therefore, claims 5, 6, 11-13, 20-22, 27, 28, and 34-36 are patentable over Timson, Moreh, and Orsini taken alone, or in combination, for at least the reasons provided above.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glen Perry

Glenn J. Perry
Attorney for Applicants
Registration No. 28,458

Date: 22 DEC 2008

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

894922_2.DOC